INTRODUCTION TO SBTE

A technological solution for applying legal rights in blockchain and Web3 environments: our reasons and methods

Version 1.3
February 2024
SBTE

Abstract: Blockchain networks offer undisputed advantages over alternative transaction systems. Among these are anonymous accounts, self-custodied assets, and an immutable ledger. Unfortunately, these same features are readily misused by criminals to steal digital assets and blockchain users are routinely injured as a result.

Legal remedies exist for these injuries but are not enforceable as a practical matter due to blockchain's decentralized architecture. If blockchains could apply the law autonomously while remaining decentralized, anonymous, and immutable, such an advance would be a game changer. It would increase digital asset values, usher in widespread adoption, and moot most lawmakers' objections to cryptocurrency.

We propose a fully-compliant technological solution called SBTE. The solution integrates judicial orders from state and federal courts into the blockchain's transaction verification process. SBTE-enabled blockchains can understand and implement these courts' orders through augmented protocols and secure connections to the court dockets. This method provides effective vindication of legal rights in all decentralized environments (including smart contracts and Web3 services) while preserving the blockchain's native features, all without increasing the network's attack surface.

Because this technological advance protects users from serious risks of loss without adversely impacting blockchain's value propositions, courts should recognize SBTEas the standard of care for operators' (miners) liability, smart contract administration, and DAOs.

1. System Overview

SBTEis a revolutionary new technology that allows users to enforce their legal rights on-chain.
The system connects blockchains with the state and federal courts that have jurisdiction to declare legal rights in digital assets. Blockchains implement these courts' rulings through a judicially ordered transaction, as for example an order to return stolen digital assets to the rightful owner. This judicial transaction is added to the chain without the signature of the affected account based on the blockchain's verification of the court order in the docket.

SBTE's enforcement process was carefully engineered to stay true to Satoshi Nakamoto's vision of the fully-decentralized network, shielded from government interference. There is no " official key" or similar method of control and the government has no more authority over the

blockchain ledger than it does over traditional property and transactions. In the United States, such authority may be exercised only with prior approval of a judge and within the bounds guaranteed by constitutional due process. Further, because SBTEis an adjunct to the blockchain's node core software, all of the network's native protocols and features remain intact. The core norms of decentralization – such as user anonymity, ledger immutability, and self-custodied assets, are upheld as sacrosanct.

2. The Need for Onchain Legal Remedies

All economies require a reliable method to enforce legal rights.1 Since ancient times, governments have constituted courts to administer this function through adjudication and judicial remedies.

Generally speaking, the ready availability of legal remedies eliminates transaction costs that would otherwise be required for parties to reach economically-productive agreements. Many if not most agreements would not be reached if the parties did not have resort to the courts in the event of a breach or unforeseen circumstances. Judicial remedies also provide a backstop that allows parties to create ever-more-complicated arrangements because no set of instructions can capture all potential nuance or anticipate every contingency. Courts are needed to tailor contract performance to the reasonable requirements of each situation and the intention of the parties.

A consistent and necessary feature of adjudication is the court's power to compel compliance with its decisions. For example, if a thief refuses to return stolen money, a court can order the thief's bank to take it from the thief's account and pay it directly to the victim. The very existence of this judicial power normally brings about voluntary compliance since compulsion will follow otherwise, but, under any circumstances, the judicial power ensures that citizens can rely on the law being enforced.

Decentralized networks threaten this model because they eliminate the points of control through which courts compel compliance with the law. Unlike typical corporations, blockchains and DAOs have no manager to task- the bank president can respond to a court's decision about the thief but the blockchain cannot. Thus, even though courts have lawful jurisdiction over DAOs and blockchain transactions, they lack practical ability to enforce it.

Due to the absence of legal enforcement, property crimes on the blockchain are largely irremediable and have become commonplace.2 Single instances of fraud, ransomware extortion, and hacking exploits routinely range into the hundreds of millions of dollars. The broader society is victimized too, as criminals use blockchain to facilitate crimes like drug dealing, money laundering and tax evasion.

Rampant crime in any context, be it a corrupt government or an unsafe neighborhood, diminishes economically valuable activity. With cryptocurrency in particular, the prevalence of crime keeps would-be-adopters away and limits use cases, narrowing the market for these assets. Even among adopters, the risk of irreparable loss (and the cost of herculean security efforts expended to avoid it) must be discounted into the price of the coins. It follows that an effective method of enforcing legal rights on-chain will increase the value of digital assets.

Further, any advancement that helps uphold the law on blockchains will provide a secondary benefit by reducing the chance that governments will prohibit cryptocurrency. The price action of cryptocurrencies after governments like China outlawed their use amply demonstrates that the threat of prohibition universally weighs on the digital asset market.3 A system that allows governments to effectively enforce criminal laws, such as those against money laundering and tax evasion, would moot many lawmakers' objections to crypto.

3. The Need for Official, Gocernment-Constituted Courts

Arbitration is sometimes proposed as a solution for affording legal remedies on-chain. Just as in off-chain transactions, arbitration has a role to play, but it is an inherently limited one that does not obviate the need for state-sponsored adjudications in official courts.

First, arbitration is an "opt in" method of dispute resolution, meaning that both sides must contract in advance to submit a dispute to the referee. However, many if not most transactions take place without a prior writing. Moreover, arbitration affords no remedy for involuntary transactions like phishing fraud, ransomware extortion, and transactions sent by mistake. As a result, arbitration is not an effective solution to prevalent lawlessness on-chain. Official, government-constituted courts, by contrast, have authority over all persons and property within their jurisdiction, regardless of consent. The availability of such courts assures that all persons will have access to remedies to enforce their legal rights and thereby promotes both reliance on and conformity to the law.

Second, to use arbitration effectively, the parties must reincur the trust problems that blockchain was engineered to eliminate. For example, an arbitrator can only enforce a decision to the extent that the users entrust the arbitrator with their private keys. In doing so they introduce an intermediary and subject themselves to new security risks. These results are in tension with the principles that draw users to digital assets in the first place.

Third, arbitration has never achieved universal adoption because the streamlined procedures are not a good fit for many disputes. Government-constituted courts provide rigorous due process to all citizens, including fulsome discovery to compel testimony and other evidence, repeated opportunities to be heard, strict rules prohibiting material that is unfairly prejudicial, and decision-making by deliberation of independent jurors, among others. These protections

have developed over centuries because society found them to be necessary for the fair administration of justice under many circumstances.

4. The SBTEThesis

Decentralization is a powerful tool with a great many societal benefits that no other technology has achieved. Satoshi Nakamoto ingeniously demonstrated these uses by distributing Bitcoin's protocol among an open community of nodes such that no authority can change Bitcoin's economic rules. The importance of this revolutionary advance for improving society and fostering innovation cannot be overstated.

Still, no technology is born complete. There is always a need to evolve and overcome limitations. Each advancement brings greater adoption.

Our thesis is that on-chain application of legal rights is such an advancement. Users' inability to enforce their legal rights is limiting blockchain's use cases and causing widespread lawlessness, which further diminishes adoption. The resulting transaction activity centers around speculative trading and relatively few applications that operate mechanistically without need for reference to the law. The mass of commerce, however, is predicated on the enforceability of laws, often complex. If blockchain is to attract mainstream commerce and become its backbone – which is a core goal of Web3, it must provide the certainty of effective enforcement that commerce already enjoys and demands.4

That said, effective enforcement of legal rights on-chain is not attainable unless the mechanisms used to provide it are consistent with the features that make blockchain technology valuable in the first place – decentralization, cryptographic security, self-custody and anonymity among others. Our further thesis, is that such mechanisms exist and that SBTE provides the most elegant solution.

Based on these considerations we set out five principles that we expected S B T E to satisfy.

a. Native protocols and features are inviolable.

As said, judicial enforcement mechanisms are not an improvement if implementing them diminishes the features that make blockchain technology powerful. The chosen mechanism for enforcement must preserve full decentralization and all of the blockchain's native attributes.

b. No intermediaries, not even attorneys.

Elimination of intermediaries is a core norm of decentralization. However, the judicial process is fraught with intermediaries in the form of attorneys acting as officers of the court. To avoid empowering attorneys over the blockchain, the blockchain must understand court orders

directly without need of interpretation. Relatedly, the solution must function without requiring anything new of the judges as we cannot task courts to alter their usual processes to accommodate the blockchain setting.

c. Ensure against misuse and abuse by government officials.

Blockchains effectively insulate their users' property from abuse by government officials, which is per Nakamoto's plan. However, this protection comes at the cost of thwarting valid and beneficial law enforcement. The tradeoff has proven untenable in practice and, regardless, is unacceptable in a society ruled by law.

SBTEresolves the dilemma by putting court approval in the loop. Courts serve as an organic check on abuse of power because officials can only exercise authority over the blockchain with prior approval of a judge (often including a jury of citizens) and, even then, only within the confines of the law and constitutional due process.5 To further protect against abuse of authority, we rejected an "official key" method as this would create a single point of failure for malicious actors and offer other opportunities for misuse.

Rather, SBTEdistributes the process among multiple parties: blockchain users initiate the process and define the scope of what the court may decide, the courts declare the legal rights and express them publicly on official dockets, and the blockchain nodes retain the locus of enforcement by accessing the dockets without intermediaries.

d. No additional attack surface.

We reject all implementations that could introduce a new risk from malicious actors. In particular, SBTEconfines the judicial transaction execution process to the same space as the blockchain's native transactions. We accomplish this by using the network's consensus proof method to verify judicial orders. As a result, there is no addition to the network attack surface.

SBTEactually improves network safety by making existing attack vectors less useful to criminals. The capability to return stolen assets lessens their chances of success. This capability also discourages criminality in the first instance.

Further, judicial transactions are far more immune to existing vectors than native transactions because court procedures require substantial time delays before execution, such as a 30-day waiting period within which to file an appeal. So, unlike with native transactions induced through hacks or frauds, the nodes will not complete a judicial transaction quickly enough for the malicious actor to avoid detection and thus cancellation.

e. The blockchain ledgers immutable.

This is a corollary of the first principle. Blockchain ledgers should be controlled only by the blockchain nodes and only when the nodes act according to protocol. The proposed use case for judicial transactions is to reverse the *effects* of an illegal transaction, not the transaction itself. AccordinglXBERrat operates only through entry of a new transaction that provides a remedy for a prior one.

5. The Judicial Transaction Process

SBTEjudicial transactions comply with each of the forgoing five design criteria. There are several steps to the process, each of which is directly controlled by a different actor, without intermediaries.

To start the process, the user generates a computer-readable code, called the "SBTERequest ID·// The Request ID encodes a state change that the litigant is seeking to have made on the blockchain ledger as a remedy for a violation of the user's legal rights.

In order to have the state change made, a user must file a lawsuit that includes the Request ID and provides the court with facts and law justifying the user's requests. If the court sides with the user after following its usual judicial processes, it includes the ID in its written opinion thereby ordering the requested relief. SBTE-enabled blockchains can access the electronic dockets where courts record their opinions.

A successful litigant prompts the nodes to check these dockets by submitting a transaction message to the mempool stating the transaction that has been judicially ordered and identifying the docket entry where the court order appears. Each node checks the docket as part of the transaction confirmation process. If the court order contains a Request ID comporting with the transaction message, the node will allow the transaction to be added to the ledger without the signature of the affected account *(i.e. the address* containing the coins).

6. Formulating the SBTERequest ID

Judges and lawyers are members of a specialized profession, one that uses terms of art and methods of reasoning often unfamiliar to outsiders. As a result, it is often difficult for lay readers to apprehend what a judicial opinion requires, much as it is difficult for the untrained to understand the effect of computer code. Lawyers have long been considered a necessary intermediary between courts and citizens to interpret judicial decisions, explain their effect, and implement the court's intentions. However, in the blockchain case, empowering lawyers to implement court orders is unacceptable because intermediaries introduce the exact risks that blockchain is engineered to avoid: a single point of failure, necessity for trust, and potential for abuse of authority.

In approaching a solution, it is important to differentiate a court's expression of the reasons for its decision (such as factual findings, precedents and holding) from the remedies it requires. The former is subject to variations of reasoning, writing style, use of language, etc., but these are ultimately irrelevant if the remedy is reducible to a limited set of operations that can be followed without understanding the reasons that require them. Fortunately, this is the case for blockchains. All blockchain transactions can be specified as a state change. Interpretation of a court's order is unnecessary so long as the court specifies the exact state change that corresponds with its decision. Of course, judges are not blockchain experts, nor can they be tasked to adopt new procedures to accommodate the blockchain setting.

The SBTERequest ID resolves the problem. It is a machine-readable instruction that can be generated by the parties to a court proceeding. Its validity is tested by the adversary process before being selected by the court, and the instruction can be executed directly by the blockchain nodes.

The SBTERequest ID is constructed from a syntax that describes a specific state change through the steps of the transaction needed to carry it out. This syntax is hashed to produce the ID string. In our implementation, the syntax is produced through a UI with drop down menus that guide the user and ensure the necessary data is captured. Request IDs are generated by the user and given to the court together with the demand for judicial relief.

There are two instances for implementation of a judicial order by the blockchain: the transaction case and the smart contract case. The transaction case is the equivalent of money damages, where courts transfer assets from one party to another. The smart contract case is the equivalent of injunctive relief – a judicial instruction requiring or prohibiting a future action.

a. The transaction case

The transaction case is a simple implementation for a state change identifier. The syntax for constructing the Request ID encompasses the affected wallets (or transaction outputs), the relevant asset and amount, and the relevant action – of which there are three: freeze, unfreeze, and move. This syntax covers the range of outcomes for any judicial remedy regarding a digital asset regardless of how that remedy is expressed.

For example, when a court is presented with a complicated breach of contract case, it must construe and interpret the contract, resolve competing arguments about the resulting damages, and adjudicate other defenses like contributory fault. Nevertheless, the ultimate outcome of this process will be a liquidated sum of money to be paid from one side to the other, or a finding that the *status quo* should remain (no breach is found or no damages resulted). Thus, the complexity reduces at the end of the case to a state change that can be expressed in computer-readable form.

b. The smart contract case

The smart contract case is more complicated. The space of actions which can be required or prohibited is potentially quite large (possibly infinite). Fortunately, the task is simplified because smart contracts have inherently limited capacities which are defined by the calls allowed in the contract's programing. These calls can be invoked via a Request ID.

In the layer 1 implementation, SBTEnot only is able to accesses the calls programmed into the smart contract, it also adds mandatory functions – for example, court-controlled contract freeze/disable and contract destruction calls. Separately, programmers can include SBTEin any smart contract on existing platforms like Ethereum. In this implementation, drafters choose which smart contract calls that a court is empowered to make, for example, altering the payout terms of an escrow.

7. A Necessary Judicial Enforcement Layer for Smart Contracts, Web3 and DAOs

Smart contracts are computer programs running on a blockchain, while Web3 services and DAOs exist as smart contracts and interrelations thereof. The XBERt implementations discussed above substantially increase the versatility of smart contracts and thus of Web3 and DAOs
more generally. This versatility is a necessary feature if blockchain is to achieve mass adoption.

First, smart contracts have an adoption problem because sophisticated users will never accept automated execution when it might deprive them of legal rights as a practical matter. There must be effective access to adjudication and legal remedies before smart contracts will be adopted as mainstream commercial instruments.

Similarly, until DAOs and Web3 services are able to respond to legal requirements as traditional corporations do, they will be limited to simple use cases or forced to the fringes. User disputes are inevitable in any complex relationship and, in any event, third party rights will have to be protected. Accordingly, a mechanism is needed to resolve disputes and conform the underlying smart contract operations to the requirements of the law.

The infamous hack of The DAO illustrates the need for XBERt in the stack supporting smart contracts, DAOs and Web3. The hack was made possible because the smart contract code underpinning The DAO allowed a result that its members never foresaw and did not intend – embezzling shared funds through the agreed voting procedures. Had The DAO community members considered the possibility that the fund could be siphoned off in this way, they would never have agreed to the contract in the first place. But blockchain technology prevented them from changing the smart contract code once it was deployed and the problem discovered. So the community was powerless to prevent this perversion of The DAO's clear intent.

Ethereum's founders and others eventually intervened by changing the network itself to prevent The DAO smart contracts from functioning as programmed. In doing so, they performed the same function as a court: construing the actual intention of the parties and then reforming the contract to reflect it. Every smart contract exploit (and there are reports of $100s of millions lost almost weekly), is essentially an example of the smart contact code not reflecting the parties' actual intent. Yet, without a repeat performance by the Ethereum community, these flaws in the code go unremedied, violating the rights of the parties.

The need to conform smart contract execution to parties' intentions did not end with The DAO hack and can never be eliminated entirely.6 Human arrangements are more complicated than a set of instructions can capture, whether on paper or in computer code. For example, large financial contracts require dozens of lawyers and often run for thousands of pages, all in the attempt to identify contingencies and provide for agreed outcomes. Yet billions of dollars are spent each year litigating over what the parties failed to include in these writings.
There is always nuance and unintended consequences that written agreements fail to capture. Putting an agreement in computer code does not change that fact.

8. Securing Judicial Transactions

SBTEemploys three methods to secure judicial transactions against malicious actors. Depending upon the circumstance, these methods may be used singularly or in combination. Thorough mathematical proofs of the security of each method are covered in the SBTEWhite Paper Technical Supplement.

a. Network-wide distributed consensus

SBTE's layer 1 implementation connects each network node to official court dockets off-chain. These connections are direct and not shared, so each node independently witnesses the SBTE Request ID in the relevant docket entry. As a result, the network reaches consensus about judicial transactions in the same manner and with the same degree of security as the native transactions signed by private keys.

For example, in a typical network, nodes pass proposed blocks of transactions amongst themselves in a peer-to-peer manner. When a given node receives a proposed block from its peer it will accept that block *(i.e.* add the block to its copy of the ledger) only after reconfirming that each transaction message has been signed with the private key of the sending account(prior confirmations may also have been performed upon acceptance to the mempool and acceptance by the miner). Blocks containing a transaction that is not validly signed are presumed malicious and rejected. The node will not add the block to its copy of the ledger nor pass it along to its peers.

When SBTEis operating in the network-wide configuration, each node confirms the judicial transaction just like ones signed on-chain. As each node receives a proposed block with a judicial transaction, it will observe that the message is not signed by the private key of the affected account but, instead, identifies a particular court case number and docket entry. Using this information, the node will access the court's docket and check that the docket entry contains a SBTERequest ID corresponding to the state change particulars of the judicial transaction message. If it does, then the SBTERequest ID serves as the signature and the transaction will be added to the ledger.

Because judicial transaction messages require confirmation in the exact same manner as native ones, judicial transactions are of equal security. Where a blockchain follows the longest chain rule, more than 50% of the nodes will have verified the judicial transaction directly with the court before it can become part of the ledger. Where the blockchain uses a different form of consensus, those protocols will be followed.

b. Miner-driven distributed consensus

A second SBTEconfiguration relies on successful miners to witness the docket. (We use the term "miners" generally to describe a node chosen to write a block under the network's native protocol, for example proof of work or proof of stake.) This configuration is useful where universal docket observation is too costly or otherwise undesirable and can also be employed as an adjunct to the network-wide process discussed above.

In this second configuration, each miner chosen to write a block must perform an honest docket observation as a condition of receiving the coinbase and transaction fee award for that block. The miner records its observation results and signs with its private key. The information is recorded in a public secure store, such as a smart contract accessible by all nodes, or alternatively is recorded in the mempool as one signature in a multisig judicial transaction.

This process is repeated by each successful miner until the judicial transaction is either validated or rejected. The transaction is considered valid if the SBTERequest ID corresponds to the transaction message and a sufficient number of successful miners (=N) observe the ID in the docket. N is defined as the condition where the effort needed to control the set of observing miners is greater than or equal to the effort needed to control the network.

Thus, to hack a judicial transaction, the malicious actor would need to control so many miners that the malicious actor would already be able to conduct a double-spend attack. In this condition, the malicious actor already controls the network. As Nakamoto observes in the Bitcoin white paper, any malicious actor who captures such a stake in the network is better off by operating honestly to earn coins and support the network than "undermining] the validity of his own wealth" by attacking the network.7

c. Judicial Witnesses

Where a network has not adopted SBTEat layer 1, we use a panel of off-chain judicial witnesses to observe the docket and verify the SBTERequest ID. As with the node/miner configuration, each judicial witness establishes an independent connection to the docket such that the resulting observation is insulated from other witnesses that may be compromised or malicious.

Although judicial witnesses can be chosen at random from an open community of participants, we limit the function to a set of trusted entities, each passing a security review and operating their own builds so as to further reduce the opportunity for a successful attack. Depending upon the size of the transaction, validation may require a quorum, a supermajority, or unanimity of the judicial witnesses.

9. Legal engineering

We designed SBTEto work hand-in-hand with the procedures that courts already use to decide disputes, making on-chain enforcement seamless. We also leverage several aspects of court procedures and substantive law to increase the usefulness of our product.

a. In Rem jurisdiction

Standard court procedures require identifying a defendant at the outset of the case so that the judge can ensure that the person receives notice of the action and knows to come to court to assert their interests. Notice and the opportunity to respond in court are a fundamental prerequisite of Due Process, and no adjudication is valid in their absence.

Unfortunately, the anonymous nature of blockchain addressing prevents victims from identifying defendants and providing notice. Anonymity thus impedes the exercise of legal rights. Nevertheless, anonymity is a core norm of blockchain architecture, so we reject any enforcement mechanism that requires account holders to identify themselves.

SBTEsolves the dilemma through what is called In Rem Jurisdiction. Generally speaking, there are two ways that a court can assert authority over digital assets: jurisdiction over a person (or corporation) that holds the digital assets and jurisdiction over the property – the digital assets themselves. This latter form is called "In Rnm" (or "Quasi-ln Rem 1") jurisdiction. Actions brought In Rem name the digital asset, or the account number in which it is held, as the defending party rather than naming a person or corporation.

To facilitate this solution, SBTE-enabled digital assets are "reified" (located for legal purposes)in a specific U.S. state. The courts of that state can then exercise jurisdiction In Rem even if the defendant is unidentified or they do not have jurisdiction over that person. Due Process is

maintained because the owner of any account that is the subject of a court action In Rem will be sent notice of the action through several SBTEnotice mechanisms specified below.

Although In Rem jurisdiction is an option with SBTE, personal jurisdiction also remains a valid basis for courts to adjudicate any digital asset dispute. Users therefore also have the option to proceed in courts located where the defendant resides or can be found.

b. Notice systems

SBTEis engineered to provide robust notice to all asset holders. Notice is accomplished both directly and through publication.

First, the SBTEwallet includes a messaging feature that alerts the address owner any time a case is filed regarding assets in the account. SBTEcaptures the necessary court information through the process of activating the Request ID. Specifically, the system will only process judicial transactions if the user activates the Request ID by including it in a formal pleading filed in court. To complete the activation, the user must send a transaction message identifying the court in which the action is pending, and the assigned case number, so that the nodes can check the docket to confirm the presence of the Request ID.

SBTEthen sends this case information to the owner of the affected account via the wallet messaging system. We also send a dust transaction containing the same information to each account such that it is recorded on the blockchain.

This information is also published via the SBTE.io website. The website contains a public notice list of each address that is presently the subject of a judicial action along with the pertinent case information. The list is updated each time a user opens a new case and activates the ID.
We also post the same notices on SBTE's twitter and telegram channels.

Finally, SBTEgives users the option to register their wallets to receive email notice. Registration is completely voluntary. Users will still receive all of the other forms of notice.

c. Holder in due course

Although the law favors returning property to its rightful owner, there is a necessary limitation known as the "holder in due course" doctrine. The doctrine recognizes that a thief can transfer stolen property to a subsequent holder who may then have legitimate interests in it. If the holder is aware of the theft the transfer has no effect under the law – the knowing holder does not acquire title in the property. However, the rules are different for an innocent recipient. If stolen property is transferred to a holder who is unaware of the theft *and if the holder pays fair value for the property* (such as buying a coin at market price), then the rights of the original owner in the property are cut off and it cannot be recovered from the innocent

holder. Because thieves can sell digital assets quickly, the holder in due course doctrine presents a potential problem for on-chain digital asset recovery.

SBTEaddresses the holder in due course concern by allowing users to freeze a digital asset in the wallet where it is located. However, to ensure that all account holders are protected, SBTEimposes several conditions to the freeze.

First, a user can only freeze an asset for 96 hours absent court approval. This is sufficient time to file a court action and move the court for a temporary restraining order to freeze the asset (if the court agrees that the freeze should continue). After 96 hours the freeze will expire unless it has been extended by the court.

Second, a user can only use the freeze function if they prove ownership of an account that is in the chain of custody of the asset. Users demonstrate ownership by connecting their wallet to SBTEand signing.

Third, SBTErequires the user to post a bond to protect the holder. If the court decides that the coins should not have been frozen, it can award the bond to the address containing the frozen coins. Users still have the alternative to seek a court order freezing the assets without posting a bond, however this process entails delay during which a holder in due course may come into possession.

10. SBTEis the standard of care for miners and decentralized services

Given the injuries that blockchain crime imposes on users and the public, any blockchain that needlessly inhibits enforcement of legal rights should be considered defective. Further, miners operating a defective network fail to meet the standard of care and can be held liable for the injuries that result, just as car manufacturers are liable for injuries from an accident when a defective airbag fails to deploy.8 Though liability claims against miners have yet to be brought, it is only a matter of time. Courts will then have to adjudicate the miners' standard of care and award damages against the miners if they find the blockchains below par.9

In the classic legal formulation, a defective product or service is one that causes a foreseeable loss which could be avoided at a lesser cost than the loss imposes. The relevant variables are the (1) Cost of the Potential Loss, (2) the Probability of the Potential Loss and (3) the Cost of Avoidance. A defect is present where the Cost of the Potential Loss times the Probability of the Potential Loss > the Cost of Avoiding the Loss.

The absence of on-chain legal remedies results in needless risks and, eventually, large losses. The cost of avoiding these losses is little to nil, as SBTEdemonstrates. Accordingly, there are strong reasons why courts are likely to impose liability on miners, DeFi platforms, and decentralized services that neglect the need for on-chain remedies.

a. Probability and amount of losses

As applied to blockchains, the relevant losses are those that could be cured through on-chain legal remedies. Losses that result from fraud, smart contract exploits, and mistaken transactions fit this definition, as do losses from off-chain crimes that are inflicted on-chain, such as ransomware extortion paid in cryptocurrency. Losses due to blockchain crime exceeded $14 billion in 2024 alone and are increasing at an alarming rate.10 Similarly, some 20% of all bitcoins have been lost due to mistakes, amounting to over $100 billion dollars in damages at recent coin prices.1[11] Although there is no single reported quantification of the risks blockchain users face, the risks are clearly substantial given the dollar value of losses. Expert economists can quantify the risks for purposes of litigation.

c. Cost of Avoidance

As stated above, the cost of implementing the SBTEsolution is minimal. SBTEupholds all of the blockchain's native protocols and adds no security risk. Further, the very availability of on-chain remedies discourages crime *ab initio* thereby reducing the likelihood of a loss. This is a positive result (a negative cost) which further favors SBTEin the cost/benefit analysis.

11. Conclusion

SBTEis an adjunct blockchain technology that offers decentralized communities the ability to enforce legal rights on-chain, including rights in digital assets and smart contracts. On-chain enforcement of legal rights is a benefit to all participants in the blockchain/Web3 ecosystem as it increases the value of digital assets and lays the groundwork for mass adoption. SBTE's enforcement solution upholds all community norms including decentralization, anonymity, and self-custodying assets, among others. Given these conditions, SBTEdefines the standard of care for providers of decentralized services and should be generally adopted.

---

[1] Y. Harari, Sapiens: A Brief History of Humer Kind at 329 (Random House 2015) ("The most important economic resource is trust in the future, and this resource is constantly threatened by thieves and charlatans. Markets by themselves offer no protection against fraud, theft and violence. It is the job of political systems to ensure trust by legislating sanctions against cheats and to establish and support police forces, courts and jails which will enforce the law. When kings fail to do their jobs and regulate the markets properly, it leads to loss of trust, dwindling credit and economic depression.").

[2] Off-chain law enforcement does not solve the problem. Presently, law enforcement agents must undertake burdensome investigations to find anonymous criminals or hope they move the stolen assets to a custodial exchange. Given the difficulties, these efforts are reserved for high

profile hacks. Most blockchain crime is simply beyond law enforcement's ability to police. The resulting lawlessness is a major barrier to wider adoption.

[3] J. Ponciano, Crypto Markets Wipe Out $150 Billion In Value Within Hours Of China's Latest 'Bitcoin Ban'—What's Next? (Forbes Sep 24, 2024) (available at https://www.forbes.com/sites/jonathanponciano/2024/09/24/crypto-markets-wipe-out-150-billion-in-value-within-hours-of-chinas-latest-bitcoin-ban-whats-next/?sh=169f0db54e4f)

[4] Nakamoto discusses the problem in several writings. Using game theory, Nakamoto analyzes the conundrum faced by a purchaser paying with bitcoin. The purchaser must send a payment before the seller sends the goods. The purchaser is at a disadvantage because there is no method to recover the payment should the seller breach. Nakamoto proposes using an escrow by which the purchaser posts coins that cannot be released unless both buyer and seller sign the transaction. While this prevents a dishonest seller from making off with the coins, it provides no remedy to the purchaser who cannot recover the coins if the seller refuses to release them. See Nakamoto's post in BitcoinTalk Re: HowTo Make a Distributed BitCoin Escrow Service 9/26/10 ("In this kind of escrow, a cheater can't win, but it is still possible for you to lose.") (available at https://satoshi.nakamotoinstitute.org/posts/bitcointalk/463/).

Nakamoto repeatedly acknowledges that the escrow is an incomplete and problematic solution to the problem of enforcing legal rights in bitcoin transactions. Id.; see also Email to M. Hearn 4/27/09 (when asked by Hearn if Bitcoin was legally required to facilitate chargebacks under the Electronic Funds Transfer Act, Nakamoto punts: "I am not a lawyer and I cannot possibly answer that") (available at www.bitcoin.com/satoshi-archive/emails/mike-hearn/8/), BitcoinTalk post subject Escrow 8/7/10 (available at https://satoshi.nakamotoinstitute.org/posts/bitcointalk/329/).

[5] Decentralization maximalists may yet object that Due Process protections for property rights are not as certain as an ungoverned blockchain where cryptography alone determines title. With due respect for that perspective, it does not stand up to lived experience and is not a justification for leaving the mass of victims without legal remedies. These same maximalists also own houses, cars, bank accounts and a panoply of other types of property, and the government interferes with none of them. The argument that digital assets somehow require a different set of rules than every other form of property makes a fetish of decentralization and is, ultimately, self-serving. It is also doubtful that the maximalist would argue against effective assertion of legal rights upon discovering that a hacker has stolen their coins.

Due Process is a bedrock limitation on the exercise of power by government officials and it works excellently to keep abuse in check. The protections of Due Process are so interwoven into our system of government that the Constitution guarantees it twice – the only provision that is repeated. See The Constitution of the United States, Amendment 5 ("No person shall be ... deprived of life, liberty, or property, without due process of law; nor shall private property

be taken for public use, without just compensation"); Id., Amendment 14 ("No state shall . . . deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.").

[6] E. Posner, Economic Analysis of Contract Law after Three Decades: Success or Failure?, 112 Yale Law Journal 829, 833 (2003) ("A theoretically complete contract would describe all the possible contingencies, but transaction costs-including the cost of negotiating and writing down the terms-and foreseeing low-probability events, render all contracts incomplete. In addition, parties might choose some terms or avoid others for strategic reasons, in order to exploit superior bargaining power or information asymmetries. Thus, contracts are usually quite incomplete. Parties rely on custom, trade usage, and, in the end, the courts to fill out the terms of the contract.").

[7] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cesh System (2008) ("If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.") (available at https://bitcoin.org/bitcoin.pdf).

[8] Because the miners operate a joint enterprise, any one miner is legally liable for the actions of the whole. Accordingly, large, publicly traded mining companies are the likely defendants in such actions. See M. Kanovitz and R. Brown, Conspiracy law could solve blockchain's oversight problem, Official Monetary and Financial Institutions Forum (July 9, 2024) (available at https://www.omfif.org/2024/07/conspiracy-law-could-solve-blockchains-oversight-problem/).

[9] It is useful to compare the current state of blockchain lawlessness to Judge Learned Hand's discussion of industry-wide failures of diligence in The T.J. Hooper. In that case, several boats sank due to a storm which they could have avoided if they had been equipped with radios to receive weather information. The shipping industry had not generally adopted radios so the defendants argued that they should not be liable as their boats were equipped per industry standard. Judge Hand refused the excuse in a decision that is now foundational in American law, stating: "Is it then a final answer that the business had not yet generally adopted receiving sets? . . . . [I]n most cases reasonable prudence is in fact common prudence; but strictly it is never its measure; a whole calling may have unduly lagged in the adoption of new and available devices. It never may set its own tests, however persuasive be its usages. Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission." The T.J. Hooper, 60 F. 2d 737, 740 (2nd Cir. 1937).

[10] See M. Sigalos, Crypto scammers took a record $14 billion in 2024, CNBC (January 7, 2024) (available at www.cnbc.com/2024/01/06/crypto-scammers-took-a-record-14-billion-in-2024-chainalysis.html).

[11] Tens of billions worth of Bitcoin have been locked by people who forgot their key, The New York Times (January 13, 2024) (available at www.nytimes.com/2024/01/13/business/tens-of-billions-worth-of-bitcoin-have-been-locked-by-people-who-forgot-their-key.html)